

Remarks

Claims 1-64 are pending. Claims 24-54 and 56-63 are withdrawn pursuant to the Examiner's previous restriction requirement.

The Examiner rejected Claims 1-33, 55 and 64 under 35 U.S.C. § 103(a) as being unpatentable over the article "Fast Inter-AP Handoff using Predictive Authentication Scheme in a Public Wireless Network." ("Choi"), in view of U.S. Patent 6,876,747 ("Faccin") and in view of U.S. Patent Application 2003/0226017 ("Palekar"). With respect to Palekar's teachings that the Examiner considers relevant to Claim 1, the Examiner states:

* * *

Choi and Faccin do not expressly mention initiating authentication of the wireless terminal (re-authentication of the wireless terminal) and communicating the data packet for immediate secure data transmission *before the authentication of the wireless terminal is completed.*

Palekar teaches initiating authentication of the wireless terminal with an authentication server and communicating immediate secure data transmission before the authentication of the wireless terminal is completed [paragraph 0051].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Palekar with Choi and Faccin to establish the TLS tunnel, since one would have been motivated to provide fast reconnect mechanism that allows wireless connections to be quickly resumed and to avoid service disruptions each time the mobile user connects to a different wireless access point [Palekar, paragraph 0010]

Applicants respectfully submits that the Examiner is mistaken. As the Examiner noted, Claim 1 recites a method by which secured data transmission is carried out immediately upon handoff and before authentication is complete:

1. A method for handoff in a wireless communication network, comprising:

generating a handoff encryption key;

handing off a wireless terminal from a first access point to a second access point; and

initiating authentication of the wireless terminal with an authentication server and communicating data packets encrypted with the handoff encryption key between the second access point and the wireless terminal for immediate secured data transmission before authentication of the wireless terminal is completed.

(emphasis added)

As explained in Applicants' Specification, at page 15, paragraphs [0060]-[0063], the above-underscored limitations allows data transmission during the handoff without perceivable interruption due to the latency of authentication with an authentication server. However, contrary to the Examiner's assertion quoted above, Palekar does not teach at paragraph [0051] "initiating authentication of the wireless terminal with an authentication server and communicating encrypted data packets between the second access point and the wireless terminal before the authentication of the wireless terminal is completed." In fact, at paragraph [0051], Palekar merely provides an abbreviated authentication procedure, which is required to be completed before encrypted communication can begin:

[0051] ... When the mobile user is then handed off to a second wireless access point, which might provide a stronger signal at the user's new location, the user's initial connection to the network would have been terminated, and the wireless access point will pass the user along to the authentication server. Rather than performing all of the steps described above, the user's computing device can, when sending the "client hello" message, include the session identifier of the previously negotiated session. The authentication server can then reference the cache and lookup the previously used cryptographic keys and other parameters for the session specified by the user's computing device. The authentication server can then respond to the user's computing device with an approval and the two can begin communicating using the previous derived cryptographic keys.

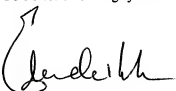
(emphasis added)

Thus, in contrast to Applicant's Claim 1, Palekar teaches communicating encrypted data packets between the second access point and the wireless terminal after the authentication of the wireless terminal is completed (i.e., approval by the authentication server obtained). Thus, the combined teachings of Choi, Faccin and Pelakar do not meet the limitations of Claim 1. Accordingly, Claim 1 and its dependent Claims 2-27 and 64 are each allowable over the combined teachings of Choi, Faccin and Pelakar. Similarly, Claims 28-33 and 55 -- which each also recite secured data transmission using a handoff encryption key occurs while an authentication process is being carried out and before completion of the authentication -- are each allowable over the combined teachings of Choi, Faccin and Pelakar. Reconsideration and allowance of Claims 1-33, 55 and 64 are therefore requested.

The Examiner provisionally rejected Claims 1-64 under the doctrine of non-statutory obviousness-type double patenting over Claims 1-25 of U.S. patent application, serial no. 10/290,650. However, as allowable subject matter has been indicated in neither this application nor the copending '650 application. Accordingly, the Examiner's rejection of Claims 1-64 is premature. Applicants will address substantively the Examiner's double-patenting rejection when the Examiner indicates allowable subject matter in this application when the Examiner indicates that the claims in this application or the copending application are allowable.

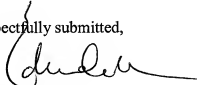
Therefore, for the reasons set forth above, all pending, examined claims (i.e., Claims 1-33, 55 and 64) are allowable over the art of record. If the Examiner has any question regarding the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant at 408-392-9250.

Certificate of Transmission: I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office (USPTO) via the USPTO's electronic filing system on July 14, 2009.

 7/14/2009

Attorney for Applicant(s) Date of Signature

Respectfully submitted,


Edward C. Kwok
Attorney for Applicant(s)
Reg. No. 33,938

Law Offices of
Haynes and Boone, LLP
2033 Gateway Place, Suite 400
San Jose, CA 95110
Tel: (408) 392-9250
Fax: (408) 392-9262